



U.S. Public Interest Research Group

National Association of State PIRGs

Board of Directors

Alaska PIRG

California PIRG

Colorado PIRG

Connecticut PIRG

Florida PIRG

Georgia PIRG

Illinois PIRG

Indiana PIRG

Iowa PIRG

Maryland PIRG

Massachusetts PIRG

PIRG in Michigan

Missouri PIRG

Montana PIRG

New Hampshire PIRG

New Jersey PIRG

New Mexico PIRG

New York PIRG

North Carolina PIRG

Ohio PIRG

Oregon State PIRG

Pennsylvania PIRG

Rhode Island PIRG

Texas PIRG

Vermont PIRG

Washington PIRG

Wisconsin PIRG

8 March 2005

The Honorable Bill Nelson (FL)
U.S. Senate
Washington, DC 20510

The Honorable Edward J. Markey (MA)
U.S. House of Representatives
Washington, DC 20515

RE: Support for The Information Protection and Security Act, S 500 and HR 1080

Dear Senator Nelson and Representative Markey,

We are writing on behalf of the state Public Interest Research Groups to endorse your House and Senate companion proposals, known as the Information Protection and Security Act (S 500 and HR 1080), responding to the Choicepoint security breach and identity theft fiasco. The act meets all the important tests of good privacy policy. It imposes Fair Information Practices (FIPs) based rules on information brokers, it allows consumers to enforce the law and it allows states to continue to enact stronger laws.

For the last 15 years, the state PIRGs¹ have been at the forefront of efforts to enact stricter rules protecting the privacy and security of confidential non-public personal information held by companies and government agencies, and by third parties, including both credit bureaus and the even less-regulated and less-known businesses known as information brokers, including Choicepoint. Of course, some of Choicepoint's products are, in fact, regulated credit reports, but how many and which ones? The company's business model is part of the problem.

While the Federal Trade Commission (FTC) has largely been a pro-privacy regulator, in our view it made two major mistakes in the 1990s that led directly to the current Choicepoint debacle. Your proposed bill is a response to the failure of both the FTC and the Congress to step up earlier to regulate information brokers.

In the early 1990s, the FTC made its first mistake, when it held that certain demographic information (names, addresses, phone numbers, Social Security Numbers) contained in credit reports and known as credit headers could be sold outside of the strict regulation of the 1970 Fair Credit Reporting Act (FCRA).

For all our concerns about the accuracy and privacy of credit reports, the FCRA remains one of our strongest privacy laws. The FCRA is largely based on the Code of Fair Information Practices. The FIPs-based FCRA limits the uses and users of credit reports, allows data

subjects (consumers) to know about, inspect and correct inaccuracies in their files, and requires data collectors to maintain the integrity and privacy of their database while subjecting them to penalties and damages for violations.

Creation of the so-called credit header loophole² helped fuel the growth of a parallel, unregulated set of commercial information brokers. The firms merge this credit header information, including Social Security Numbers, with increasingly available public record information collected and assimilated from anyplace the companies could find it. The firms also layer marketing preference data on top of the public record and credit data to enhance their profiling efforts.

Their collection and aggregation of these data violate one of the most important of the FIPs: Information collected for one purpose should not be used for any secondary purpose without the data subject's consent.³ The failure of information brokers to allow the consumers/citizens who are their data subjects access to or even knowledge of their files violates another of the FIPs: there shall be no secret databases.

As its second mistake, in the late 1990s, instead of calling for regulations or Congressional action, the FTC officially encouraged self-regulation⁴ of the rapidly growing information broker industry, then-organized as the (apparently now-defunct) Individual Reference Services Group.

So, on the one hand, Congress in 1970 enacted the FCRA, strictly regulating commercial and government use of credit reports, and strengthened that law in both 1996 and 2003. Yet, on the other hand, under advice from the FTC and pressure from the politically-powerful information broker companies, Congress declined to similarly regulate the growing parallel universe of data held by these so-called information brokers.

Unfortunately, as hearings will point out, there is probably a vast co-mingling of data, the data in the two universes are used for similar decision-making and, as the Choicepoint debacle further points out, misuse of the data or failure to keep it accurate, regardless of which universe it comes from, leads to the same harsh realities for consumers—identity theft, stalking, misidentification as a criminal⁵ or denial of necessary services, ranging from credit, insurance or access to government programs.

Your legislation, **The Information Protection and Security Act, S 500/HR 1080**, is an important step toward reform. The proposed bill would:

- Subject Choicepoint and other information brokers to FIPs-based rules to be issued by the FTC within six months;
- Require information brokers to better secure the information they hold, grant consumers the right to obtain access to and correct their files, require information brokers to protect information from unauthorized users and prohibit users of an information broker to obtain information for impermissible or unlawful purposes.

Importantly, your legislation also takes two other critical approaches that have been largely rejected by Congress in recent privacy legislation.

- First, it allows consumers to enforce violations of the proposed law through a private right of action.
- Second, it preserves the right of the several states, the laboratories of democracy, to enact stronger privacy laws provided that they are not inconsistent.

In 2003, when Congress enacted comprehensive FCRA amendments known as the Fair and Accurate Credit Transactions Act (FACTA), it largely rejected both of these important principles.

Most egregiously, of course, Congress had actually ignored the identity theft epidemic completely for many years. In 2003, the driving force toward enactment of FACTA was not any increase in the intensity of identity theft, rather, it was the pending expiration of temporary 1996 limits on some state authority under the FCRA.⁶ The powerful credit industry labored mightily to expand and make those limits permanent with passage of the FACTA, but was unable to prevent some consumer reforms from being included in the new law, including the right to a free credit report annually, the right to disclosure of credit scores, the right to effective fraud alerts and the right for identity theft victims to obtain information needed to clear their names. Nearly all of FACTA's reforms were derived from previous state legislation.

While we were unable to stop the extension and expansion of most limits on state authority, or to provide consumers with a private right of action for FACTA violations, PIRG and other advocates were successful in protecting state authority to enact stronger laws in a number of areas related to identity theft.

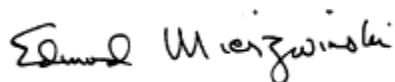
Were it not for California's previous enactment of security breach disclosure legislation, for example, we would not have found out about the Choicepoint fiasco. A dozen states or more are now considering security breach proposals, security freeze proposals (which allow consumers to "freeze" access to their reports to new users, and have already been enacted in California, Texas, Louisiana and Vermont) and other reforms⁷. So, we commend you for preserving state authority to make stronger laws against information brokers.

Federal law should always serve as a floor, not a ceiling. If Congress does a good enough job, industry has no worry at all of so-called "balkanization." If, however, Congress does a less adequate job, then states can respond quickly to new privacy problems. Otherwise, we would likely have to wait for yet another scandal to convince Congress to act again.

Recall that even Enron wasn't a large enough scandal to move the Congress to enact corporate reform, it also took Worldcom. We can only hope that the Choicepoint scandal, with the added impetus of the Bank of America breach, equals enough of a "privacy Enron" or a "privacy Valdez" to drive your reasoned and thoughtful legislation to final passage. It meets all the important tests of good privacy policy. It imposes FIPs-based rules on an unregulated parallel universe of data brokers, it allows consumers to enforce the law and it allows states to continue to enact stronger laws.

Please have your staff contact me at 202-546-9707 x314 if you have any questions. We look forward to working with you on this and other important legislative initiatives to protect consumer and citizen privacy in the 21st century.

Sincerely yours,



Edmund Mierzewski
Consumer Program Director

¹ See PIRG's website on identity theft and credit reporting, for links to all of our reports and advocacy efforts and to our "state model law on identity theft," at <http://www.pirg.org/consumer/credit> See the PIRG consumer testimony page for our Congressional testimony on privacy issues <http://www.pirg.org/consumer/testimony.htm>

² Congress should also affirmatively shut this credit header loophole. While the Gramm-Leach-Bliley regulations on financial privacy (FTC Final Privacy Rule 16 CFR Part 313 "Privacy Of Consumer Financial Information," 12 May 2000) provide that credit headers can only be sold with "notice and opt-out," those regulations do not affirmatively or completely close off sale of credit headers. See discussion pages 79-82 at <http://www.ftc.gov/os/2000/05/glb000512.pdf>

³ Since Choicepoint and other information brokers sell to both commercial firms and government agencies, data subjects can be consumers, citizens, or both.

⁴ The Nexis-Lexis Privacy Policy states that "The IRSG consulted with the FTC in formulating its principles and auditing measures, and the FTC approved these principles and audit measures." See <http://www.lexis-nexis.com/clients/iip/dataPrivacy.htm> Also see "Individual Reference Services: A Report to Congress," FTC, October 1997, which states "The Commission commends members of the IRSG Group for the commitment and concern they have shown in drafting and agreeing to comply with an innovative and far-reaching self-regulatory program." <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm>

⁵ Law enforcement agencies obtain information from commercial information brokers that they may otherwise be restricted from collecting directly. Further, if it is inaccurate, data subjects could be wrongly classified as criminals, or terrorists. See Hoofnagle, Chris Jay, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement" University of North Carolina Journal of International Law & Commercial Regulation, Summer 2004 <http://ssrn.com/abstract=582302>

⁶ See Mierzewski, Edmund, "Preemption Of State Consumer Laws: Federal Interference Is A Market Failure," which appeared in the Spring 2004 (Vol. 6, No. 1, pgs. 6-12) issue of the Government, Law and Policy Journal of the New York State Bar Association. Available at <http://www.pirg.org/consumer/pdfs/mierzewskiarticlefinalnysba.pdf> The article discusses the history of the FACT Act and other state preemption issues in detail. For an archive of PIRG materials on the need for stronger state consumer laws, see <http://www.stopatmfees.com/occpirg.htm>

⁷ See the PIRG/Consumers Union State Model Identity Theft Law, The State Clean Credit and Identity Theft Protection Act, available at <http://www.pirg.org/consumer/credit/model.htm>.